UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MARY JANE WHALEN, Individually and On Behalf of All Others Similarly Situated, Plaintiff, v. MICHAEL STORES INC., Defendant.	No. CLASS ACTION COMPLAINT JURY TRIAL DEMAND

Plaintiff Mary Jane Whalen ("Plaintiff" or "Whalen") brings for her class action complaint on behalf of herself and all others similarly situated, upon personal knowledge as to the facts pertaining to her and upon information and belief as to all other matters, based on investigation of her counsel, against defendant Michaels Stores Inc. ("Defendant" or "Michaels"), and states as follows:

NATURE OF ACTION

This is a consumer class action for damages and injunctive relief against Defendant for damages sustained by Plaintiff and other members of the putative class as a result of Defendant's failure to maintain the security of the financial and personal information of Defendant's credit and debit card customers at Defendant's stores in the United States. Defendant is liable for damages to Plaintiff and the Class for inadequate security of Plaintiff's sensitive personal and financial data against intrusion and breach of security.

INTRODUCTION

1. On January 25, 2014, Michaels initially disclosed a possible data breach involving the theft of customers' credit-card and debit-card data (the "Security Breach"). While the

existence of the breach was allegedly uncertain to Defendant, Michaels had previously been alerted to "possible fraudulent activity on some U.S. payment cards that had been used at Michaels."[1]

2. On April 17, 2014, Michaels CEO Chuck Rubin confirmed the Security Breach and divulged more details regarding its breadth and scope.[2] Reportedly, approximately 3 million customers had their personal information compromised by the breach when making purchases at both Michaels stores and Aaron Brothers stores, a subsidiary of Michaels.

3. Michaels' security failures enabled the hackers to steal financial data from within Michaels' stores and subsequently make unauthorized purchases on customers' credit cards and otherwise put Class members' financial information at serious and ongoing risk. The hackers continue to use the information they obtained as a result of Michaels' inadequate security to exploit and injure Class members across the United States.

4. The Security Breach was caused and enabled by Michaels' knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. Michaels grossly failed to comply with security standards and allowed their customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

5. Michaels failed to disclose the extent of the Security Breach and notify its affected customers of the Breach in a timely manner. Michaels failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Security

---

[1] Chuck Rubin, *A Letter From Our CEO*, Michaels (Jan. 25, 2014), http://www.michaels.com/corporate/payment-card-notice,default,pg.html.

[2] Chuck Rubin, *A Letter From Our CEO*, Michaels (Apr. 17, 2014), http://www.michaels.com/corporate/payment-card-notice-CEO,default,pg.html.

Breach. Furthermore, by failing to provide adequate notice, Michaels prevented Class members from protecting themselves from the Security Breach.

6. Accordingly, Plaintiff, on behalf of herself and other members of the Class, asserts claims for breach of implied contract and violation of the New York General Business Law § 349 and similar consumer fraud statutes, and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

Plaintiff Whalen

7. Mary Jane Whalen is a citizen of the State of New York and is domiciled in Nassau County, New York. Whalen made purchases with her credit card at a Michaels retail location in Manhasset, NY, on December 31, 2013. As a result, Whalen entered into an implied contract with Michaels for the adequate protection of her credit card information and had her sensitive financial information exposed as a result of Michaels' inadequate security. Thereafter, on January 14, 2014, Whalen's credit card was physically presented for payment to a gym in Ecuador for a charge of $398.16. On January 15, 2014, Whalen's credit card was also physically presented for payment to a concert ticket company in Ecuador for a charge of $1,320.00. Whalen has never been to Ecuador, did not give her card to someone who travelled to Ecuador, and did not authorize for payments to be made in Ecuador. Whalen canceled her card on January 15, 2014. On information and belief, physical presentment of a card is only possible by recreating a credit card with stolen PII, and, therefore, Whalen's card was fraudulently recreated and used in Ecuador.

8. Ms. Whalen reasonably believed Defendant would safeguard her financial information in its payment process. Ms. Whalen was never informed that Defendant would retain

her credit card information. Ms. Whalen never consented to allow Defendant to collect the information from her credit card much less agree to have that PSI retained by Defendant for any purpose.

Defendant Michaels

9. Defendant Michaels Stores Inc. is a Delaware corporation with principal offices at 800 Bent Branch Drive, Irving, Texas 75061. Michaels is the largest arts and crafts specialty retailer in North America providing materials, project ideas, and education for creative activities. Defendant does substantial business in New York. Michaels owns and operates stores throughout the United States.

VENUE AND JURISDICTION

10. Venue in this Court is proper because a substantial part of the acts or omissions giving rise to the claims in this action occurred in this Judicial District.

11. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) the class has more than 100 members, (b) at least one of the members of the proposed class is a citizen of a state other than New York, and (c) the total amount in controversy exceeds $5 million exclusive of interest and costs.

12. This Court has personal jurisdiction over Defendant because a substantial portion of the wrongdoing alleged in this Complaint took place in this District and Defendant is authorized to do business in this District, has sufficient minimum contacts with this District, and/or otherwise intentionally avails itself of the markets in this District through the promotion, marketing and sales in this District so that the exercise of personal jurisdiction of this Court complies with judicial notions of fair play and substantial justice.

GENERAL ALLEGATIONS

The Data Breach

13. Michaels operates approximately 1,106 retail locations in 49 states and Canada, and Michaels also operates 123 Aaron Brothers stores in nine states. Like many other retailers, Michaels processes in-store debit and credit card payments.

14. At this point, Michaels has confirmed that approximately 3 million consumers became the victims of a data breach when their personal information was taken from Michaels' payment card information systems as a result of malicious software. Approximately 2.6 million cards were compromised at Michaels stores during a breach which lasted almost 9 months from May 8, 2013 to January 27, 2014.

15. Furthermore, approximately 400,000 cards were compromised at various Aaron Brothers stores during a breach lasting around 8 months, from June 26, 2013 to February 27, 2014.

16. Michaels has received reports of fraud from payment card brands and banks relating to the fraudulent use of cards connected to Michaels and Aaron Brothers.[3]

17. Furthermore, almost *one year* has passed from the beginning of the data breach to Michaels' confirmation of the breach. In addition, nearly three months passed between when Defendant originally notified the public of a possible breach and when Defendant affirmatively confirmed that the Breach occurred.

18. Michaels' failure to comply with reasonable security standards provided Michaels with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of Michaels' own customers – including Class members here

[3] *See supra*, note 2.

– who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

19. Moreover, this breach is the second time in the past three years that Michaels has been the subject of a security breach. The prior incident occurred in May 2011 and should have alerted Michaels of the need for additional security measures.

20. Michaels allowed widespread and systematic theft of its customers' financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

Security Breaches Lead to Identity Theft

21. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[4] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

22. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history, and reputation and can take time, money, and patience to resolve.[5] Identity thieves use stolen personal information for a variety of crimes, including credit

[4] *See* http:///www.gao.gov/new.items/d07737.pdf.
[5] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Dec. 19. 2013).

card fraud, phone or utilities fraud, and bank/finance fraud.[6]

23. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

24. Personal identifying information ("PII") – such as Michaels' customer names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action– is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[7] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, and other PII directly on various Internet websites making the information publicly available.

25. This information can be sold on the black-market almost immediately. As Illinois Attorney General Lisa Madigan aptly put it, "the second somebody gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black market and someone's

---

[6] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

[7] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009).

starting to make unauthorized transactions."[8]

26. Moreover, this card information can be worth as much as $45 on the black market, according to the New York Times reporting on the Target data breach:

> The black market for credit card and debit card numbers is highly sophisticated, with numerous card-selling sites that are indistinguishable from a modern-day e-commerce site. Many sell cards in bulk to account for the possibility of cancellations. Some go for as little as a quarter apiece. Corporate cards can sell for as much as $45.[9]

The Monetary Value of Privacy Protections

27. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[10]

28. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[11] For example, supermarket operator Kroger Co. records what customers buy at its more than 2,600

---

[8] Phil Rosenthal, *Don't wait to be a cybertheft victim*, Chi. Trib., Oct. 1, 2014, at 1.

[9] Elizabeth A. Harris, *In Apology, and a Sale, Target Tries to Appease*, N.Y. Times (Dec. 20, 2013), http://www.nytimes.com/2013/12/21/business/in-apology-and-a-sale-target-tries-to-appease.html?_r=0

[10] *The Information Marketplace: Merging and Exchanging Consumer Data*, http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (last visited Dec. 20, 2013).

[11] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Dec. 20, 2013) ("Web's Hot New Commodity: Privacy").

stores. Then, Kroger sifts through this data and sells that information for upwards of $100 million annually.[12]

29. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[13]

30. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PII.[14] This business has created a new market for the sale and purchase of this valuable data.[15]

31. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

32. Personal and financial information such as that stolen in the Michaels data breach is highly coveted by and a frequent target of hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or

---

[12] Vipal Monga, *What Is All That Data Worth?*, Wall St. J., Oct. 13, 2014, at B1.

[13] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Dec. 20, 2013).

[14] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited Dec. 20, 2013).

[15] *See Web's Hot New Commodity: Privacy.*

[16] *Signs of Identity Theft*, FTC (July 2012), http://www.consumer.ftc.gov/articles/0271-signs-identity-theft.

maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts.

33. The ramifications of Michael's failure to keep customer's personal and financial information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes.

34. Identity thieves can use personal information, such as that pertaining to the Plaintiff and the Class, which Michaels failed to keep secure, to perpetuate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

35. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

[17] Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added) (last visited Dec. 20, 2013); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

36. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website.[18]

37. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Michaels Failed to Comply with Relevant Industry Standards for Data Security

38. The point-of-sale devices tampered with in the Michaels breach are known to be especially vulnerable. In August 27, 2007, Dr. Neal Krawetz of Hacker Factor Solutions publicly disclosed a white paper titled "Point-Of-Sale Vulnerabilities"[19] (the "White Paper"). The White Paper abstract described its content as follows:

> Point-of-Sale (POS) systems provide the initial interface for credit card transactions. While the communications between POS systems have been hardened through the use of cryptography and a variety of authentication techniques, the devices themselves provide virtually no security. Pew POS systems implement best practices for handling sensitive information, such as the Visa standards for credit card management. This document describes common risks to credit card users due to POS systems.

39. The White Paper then provided a detailed description of the typical POS system and its components, including the "5.2.2 Lax security processes" and "5.3 Security up for Auction." The White Paper described POS "Branch Servers" and how their vulnerability could result in the compromise of millions of credit card accounts.

40. In his conclusion for the White Paper, Dr. Krawetz notes:

> Point-of-sale terminals and branch servers store credit card information in ways that are no longer secure enough. These

---

[18] *Id.*

[19] Dr. Neal Krawetz, *Point-of-Sale Vulnerabilities*, Hacker Factor (2007), http://www.hackerfactor.com/papers/cc-pos-20.pdf

> vulnerabilities are not limited to any single POS vendor; they pose a fundamental hole in the entire POS market. It seems that nearly every POS provider is vulnerable, including Verifone, Fujitsu Transaction Solutions, Retalix, Hypercom, Autostar, Innovax, IDA, JPMA, NCR, StoreNext, IBM, and Systech. Similarly, these vulnerabilities impact all retailers that use these systems, including (but not limited to) OfficeMax, BestBuy, Circuit City, Target, Wal-Mart, REI, Staples, Nordstrom, and Petco. The amount of vulnerability varies between retailers and their implementations. But in general, if a credit card is not required to return a product, or the product can be returned at any store, then the retailer likely has a serious vulnerability.

41. Dr. Krawetz summarizes the vulnerable aspects of the POS architecture, including Branch Servers and closes:

> Even though other sightings have occasionally surfaced, the February 9th [2006] announcement showed the first big vendor being publicly hit with this problem. This compromise was not the first, it is unlikely to be the last, and it certainly will not be the biggest. **It is only a matter of time before a national branch server at a large retailer is compromised.** (Emphasis added.)

42. On information and belief, Michaels did not implement the suggestions in the White Paper.

43. In addition, members of the payment card industry ("PCI") established a Security Standards Counsel ("PCI SSC") in 2006 to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

44. The PCI DSS provides, "PCI DSS applies to all entities involved in payment card processing—including merchants."[20] Michaels is a merchant that accepts payment cards.

45. The PCI DSS requires a merchant to, among other things, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test networks.

---

[20] *Requirements an Security Assessment Procedures, Version 3.0*, Payment Card Industry DataSecurityStandard,at5(Nov2013),https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

46. Furthermore, financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants such as Michaels must take to ensure that valuable transactional data is secure and protected. The debit and credit card companies issue regulations ("Card Operating Regulations") that bind Michaels as a condition of its contract with the bank. The Card Operating Regulations prohibit Michaels and other merchants from disclosing any card holder account numbers, personal information, magnetic stripe information or transaction information to third parties (other than the merchant's agent, the acquiring bank, or the acquiring bank's agents). The Card Operating Regulations further require Michaels to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

47. On information and belief, Michaels failed to comply with the PCI DSS as well as Card Operating Regulations, resulting in the security breach.

Damages Sustained By Plaintiff and the Class

48. A portion of the services purchased from Michaels by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products purchased from Michaels.

49. Plaintiff and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts. As detailed above, Plaintiff incurred

specific unauthorized activity in her account and incurred specific unauthorized charges as a direct result of the Security Breach.

50. After the breach, Michaels encouraged consumers to check their credit reports, place holds on their credit reports, file police reports, and close any affected accounts.[21] However, as explained above, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

51. Despite this protracted period of potential fraud, Michaels offers affected consumers only one year of credit monitoring.[22] As security blogger Brian Krebs notes, "credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts – such as credit and debit cards – and they're not great at stopping new account fraud committed in your name."[23] Michaels' proposed solutions to the potential fraud are, therefore, woefully deficient.

52. As a result of these activities, Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Michaels' wrongful conduct, particularly given the incidents of actual misappropriation from Class members' financial accounts, as detailed above.

53. Moreover, for customers of credit unions, this breach and the resulting fraud will raise the cost of credit. As one executive at Mission Federal Credit Union noted, because credit unions are non-profits, "when [credit unions] take $100,000 in credit card losses [resulting from fraudulent charges], that's $100,000 that we could have used to give our customers higher interest

---

[21] *Additional Information*, Michaels, http://www.michaels.com/corporate/payment-card-notice-info,default,pg.html (last visited Mar. 31, 2014).

[22] *See supra*, note 2.

[23] Brian Krebs, *3 Million Customer Credit, Debit Cards Stolen in Michaels, Aaron Brothers Breaches,* Krebs on Security (Apr. 14, 2014), http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/#more-25704.

rates or lower loan rates."[24] Even if a customer is not responsible for fraudulent charges, then, a data breach resulting in such fraudulent charges will nonetheless raise the cost of acquiring credit by all customers of credit unions, further damaging them.

54. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings Count I, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in the United States who made an in-store purchase at a Michaels store using a debit or credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the "National Class").

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. Plaintiff brings Count II, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[25] who made an in-store purchase at a Michaels store using a debit or

[24] Elizabeth Weise, *Massive data breaches: Where they lead is surprising*, U.S.A. Today (Oct. 3, 2014 10:30 AM), http://www.usatoday.com/story/tech/2014/10/02/home-depot-data-breach-credit-card-fast-food/16435337/

> credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the "Consumer Fraud Multistate Class").

Excluded from the Consumer Fraud Multistate Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

57. In the alternative to Count II, Plaintiff brings Count III, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of the following two state sub-classes, defined as:

> All persons residing in the State of New York who made an in-store purchase at a Michaels store using a debit or credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the "New York State Class").

Excluded from the New York State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

58. The National Class, Consumer Fraud Multistate Class, and New York State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

59. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

---

[25] The States in the Consumer Fraud Multi-State Class are limited to those States with similar consumer fraud laws under the facts of this case: California (Cal. Bus. & Prof. Code §17200, *et seq.*); Florida (Fla. Stat. §501.201, *et seq.*); Illinois (815 Ill. Comp. Stat. 502/1, *et seq.*); (Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws §445.901, *et seq.*); Minnesota (Minn. Stat. §325F.67, *et seq.*); Missouri (Mo. Rev. Stat. 010, *et seq.*); New Jersey (N.J. Stat. §56:8-1, *et seq.*); New York (N.Y. Gen. Bus. Law §349, *et seq.*); and Washington (Wash. Rev. Code §19.86.010, *et seq.*).

60. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Michaels' books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

61. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Michaels failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;

b. Whether Michaels properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;

c. Whether Michaels' conduct violates the New York and other asserted Consumer Fraud Acts;

d. Whether Michaels' conduct constitutes breach of an implied contract;

e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

62. Michaels engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

63. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Michaels' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Michaels that are unique to Plaintiff.

64. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation; and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and her counsel.

65. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Michaels. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

66. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Michaels has acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

67. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Michaels, so it would be impracticable for Class members to individually seek redress for Michaels' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS ALLEGED

COUNT I
Breach of Implied Contract
(On Behalf of the National Class)

68. Plaintiff hereby incorporates by reference each paragraph of this Complaint, as if fully set forth herein.

69. Michaels' customers who intended to make in-store purchases with debit or credit cards were required to provide their card's magnetic strip data for payment verification.

70. In providing such financial data, Plaintiff and the other members of the Class entered into an implied contract with Michaels whereby Michaels became obligated to reasonably safeguard Plaintiff's and the other Class members' sensitive, non-public information.

71. Plaintiff and the Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract.

72. Michaels breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

73. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money, and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
Violation of N.Y. Gen. Bus. Law § 349
(and Substantially Similar Laws of the Consumer Fraud States[26])
(on Behalf of the Consumer Fraud Multistate Class)

74. Plaintiff hereby incorporates by reference paragraphs 1-67 of this Complaint, as if fully set forth herein.

75. Defendant's transactions with Plaintiff and the Class as described herein constitute the "conduct of any trade or commerce" within the meaning of NYS GBL § 349.

76. Defendant in the normal course of their business collected customer information stating that such data was for the immediate financial transactions.

77. Plaintiff and the other members of the Class were deceived by Michaels' failure to properly implement adequate, commercially reasonable security measures to protect their

[26] The Consumer Fraud States were defined at *supra* note 19.

private financial information while shopping at Michaels.

78. Michaels intended for Plaintiff and the other members of the Class to rely on Michaels to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

79. Defendant misrepresented the safety and security of their payment systems, and the unauthorized collection and storage of customer financial information beyond the immediate transaction.

80. Michaels instead handled Plaintiff and the other Class members' personal information in such manner that it was compromised.

81. Michaels failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

82. It was foreseeable that Michaels' willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

83. Michaels benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Michaels saved on the cost of those security measures.

84. Michaels' fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Michaels' deception that their financial information was secure and protected when using debit and credit cards to shop at Michaels.[27]

85. The foregoing acts and conduct of Defendant are deceptive in that it represented

[27] The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

to the consumer class that such information of the immediate transaction would remain secure and/or that it had the technology or policies to secure financial transaction information when Defendant did not have adequate security measures.

86. The foregoing acts and conduct of Defendant are deceptive in that Defendant represented that its acts were necessary solely for the financial transaction at the time of purchase, not for data collection purposes.

87. The foregoing acts and conduct of Defendant are harmful in that Defendant did not in fact have adequate security in place to secure the financial and sensitive personal information of Plaintiff and the Class.

88. Michaels' acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a)

89. By these deceptive acts, Defendant caused harm to Plaintiff and the Class.

90. Plaintiff and the other Class members' injuries were proximately caused by Michaels' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

91. By this conduct, Michaels violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of New York, or conflict with each other for purposes of this action.

COUNT III
Violation of New York General Business Law
(In the alternative to Count II and on behalf of the New York State Class)

92. Plaintiff hereby incorporates by reference paragraphs 1-67 of this Complaint as if fully set forth herein.

93. New York General Business Law ("GBL") § 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce." N.Y. Gen. Bus. Law § 349.

94. Defendant's transactions with Plaintiff and the Class as described herein constitute the "conduct of any trade or commerce" within the meaning of GBL § 349.

95. Defendant in the normal course of its business collected customer information.

96. Michaels violated GBL § 349 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other members' private financial information, by failing to warn shoppers that their information was at risk, and by failing to immediately notify affected customers of the nature and extent of the security breach. Defendant misrepresented the safety and security of their payment systems, and the unauthorized collection and storage of customer financial information beyond the immediate transaction.

97. Plaintiff and the other members have suffered injury in fact and actual damages including lost money and property as a result of Michaels' violations of GBL § 349.

98. Plaintiff's and the other Class members' injuries were proximately caused by Michaels' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all the claims asserted.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Michaels, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering Michaels to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering Michaels to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

D. Ordering Michaels to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Ordering Michaels to pay statutory damages, as provided by the New York General Business Law § 349 and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;

F. Ordering Michaels to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;

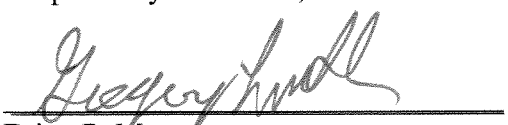
G. Ordering Michaels to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Ordering Michaels to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Dated: December 2, 2014

Respectfully submitted,



Brian P. Murray
bmurray@glancylaw.com
Gregory B. Linkh
glinkh@glancylaw.com
GLANCY, BINKOW AND GOLDBERG LLP
122 E 42nd Street, Suite 2920
New York, NY 10168
Tel: 212.682.5340
Fax: 212.884.0988

Joseph J. Siprut
jsiprut@siprut.com
Gregory W. Jones
gjones@siprut.com
SIPRUT PC
17 North State Street
Suite 1600
Chicago, Illinois 60602
312.236.0000
Fax: 312.267.1906

Daniel A. Edelman
courtecl@edcombs.com
Rebecca A. Cohen
rcohen@edcombs.com
EDELMAN, COMBS, LATTURNER & GOODWIN LLC
120 S. LaSalle
Suite 1800
Chicago, Illinois 60603
312.739.4200
Fax: 312.419.0379

Mark T. Lavery
mark@lifetimedebtsolutions.com
HYSLIP & TAYLOR LLC LPA
917 W. 18th Street
Suite 200
Chicago, Illinois 60608
312.508.5480

Christopher V. Langone
207 Texas Lane
Ithaca, NY 14850
607.592.2661

Katrina Carroll, Esq.
kcarroll@litedepalma.com
LITE DEPALMA GREENBERG, LLC
Chicago Office
One South Dearborn
Suite 2100
Chicago, Illinois 60603
312.739.4200
Fax: 312.419.0379

Robert Ahdoot

rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, P.C.
1016 Palm Avenue
West Hollywood, CA 90069
310.474.9111
Fax: 310.474.8585

John A. Yanchunis
jyanchunis@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602
813.275.5272
Fax: 813.226.5402

Richard R. Gordon
richard.gordon@gordonlawchicago.com
GORDON LAW OFFICES, LTD.
211 West Wacker Drive
Suite 500
Chicago, Illinois 60606
312.332.5200
Fax: 312.236.7727